

## REMARKS

### 1. 35 U.S.C. § 112. Rejections.

Claim 6 and Claim 21 are rejected under 35 U.S.C. §112, second paragraph.

5 As to Claim 6 and Claim 21, line 3, the Office Action states that “there is no antecedent basis for “said entered private key”.

Applicant has amended dependent Claim 6, Claim 7, and Claim 8, to claim an “assigned private key”, which provides proper antecedent basis to the assigned private key, as claimed in independent Claim 1.

Applicant has also amended dependent Claim 21, Claim 22, and Claim 23, to claim an “established private key”, which provides proper antecedent basis to the established private key, as claimed in independent Claim 16.

Applicant therefore respectfully submits that Claim 6 and Claim 21, as amended, overcome the rejections under 35 U.S.C. §112, second paragraph.

### 2-3. 35 U.S.C. § 102. Rejections.

20 3. Claims 1, 3-6, 8, 9, 11, 13-15, 16, 18-21, 23, 24, 26, and 28-30 are rejected under 35 U.S.C. §102(e) as being anticipated by Franklin et al (U.S. Patent No. 6,000,832).

3a. Regarding Claims 1, 9, 15, 16, 24 and 30, the Office Action states that “Franklin et al teach an electronic online commerce card such that Applicant’s certificate authority reads on element 32 and column 9, lines 4-11, Applicant’s virtual certificate reads on the electronic online commerce card, Applicant’s redemption denomination reads on the customer’s credit/debit limit, Applicant’s first public key identifier reads on the inherent public key which would correspond to the assigned private key , column 2, lines 17-19 and column 8, lines 21-24, Applicant’s certificate issuance module reads on the software module used to formulate transaction numbers, Applicant’s certificate including redemption denomination and first public key identifier reads on the customer’s credit card/debit card and column 8, lines 21-24 respectively, Applicant’s storing of redemption denomination, first public key identifier and private key reads on

the customer database, element 62, Applicant's authenticating module reads on the issuing institution and column 2, lines 51-55, and Applicant's canceling means reads on the inherent rejection of the authorization request if the customer data in the request is not correct."

5

Applicant has amended independent Claim 1, to claim a certificate system on a network, comprising:

a certificate authority connected to said network, said certificate authority adapted to allow the definition of a virtual certificate comprising a redemption  
10 denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

a certificate issuance module for creation of an issued certificate upon selectable acquisition of said virtual certificate by an acquirer user across said network, said issued certificate comprising said redemption denomination and  
15 said first public key identifier, said creation of said issued certificate comprising a private key assigned at time of said acquisition of said virtual certificate, wherein said redemption denomination, said first public key identifier, and said assigned private key are stored at said certificate authority in association with said issued certificate;

20

a certificate authentication module for authorization of an off-line redemption of said issued certificate at a redemption location to a holder of said issued certificate located at said redemption location, based upon a communication from said remote location to said certificate authority of said redemption denomination and said first public key identifier from said issued  
25 certificate, and said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

25

means to cancel further redemption of said issued certificate at said certificate authority.

30

Applicant has also amended independent Claim 16, to claim a process within a transaction network, comprising the steps of:

defining a virtual certificate on a certificate authority, said defined virtual certificate comprised of a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

creating an issued certificate upon acquisition of said virtual certificate by an acquirer user on said transaction network, said issued certificate comprising said redemption denomination and said first public key identifier, said creation of said issued certificate comprising an establishment of a private key, said redemption denomination, said first public key identifier, and said established private key stored at said certificate authority in association with said issued certificate;

authorizing an off-line redemption of said issued certificate at a redemption location to a holder of said issued certificate, based upon redemption submittal at said redemption location of said redemption denomination and said first public key identifier from said issued certificate, and said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

canceling further redemption of said issued certificate at said certificate authority.

Support is seen in the Application as filed, as least on page 7, lines 6-26; on page 9, line 10 to page 10, line 12; on page 11, lines 1-23; on page 13, line 6 to page 14, line 29; on page 23, lines 8-16; on page 26, line 20 to page 27, line 29; in Figure 1 to Figure 4, and in Figure 8.

While Franklin et al describe an electronic online commerce card with customer generated transaction proxy number for online transactions, Applicant respectfully submits that the online commerce card described by Franklin is significantly different than the present invention, as claimed in Claim 1 and Claim 16, as amended. An overview of the electronic online commerce card, as disclosed by Franklin et al, is seen at least in the Abstract, wherein:

"An online commerce system facilitates online commerce over a public network using an online commerce card. The "card" does not exist in physical form, but instead exists in digital form. It is assigned a customer account number that includes digits for a prefix number for bank-handling information, digits for a customer identification number, digits reserved for an embedded code number, and a digit for check sum. The bank also gives the customer a private key. During an online transaction, the customer computer retrieves the private key and customer account number from storage. The customer computer generates a code number as a function of the private key, customer-specific data (e.g., cardholder's name, account number, etc.) and transaction-specific data (e.g., transaction amount, merchant ID, goods ID, time, transaction date, etc.). The customer computer embeds the code number in the reserved digits of the customer account number to create a transaction number specific to the transaction. The customer submits that transaction number to the merchant as a proxy for a regular card number. When the merchant submits the number for approval, the issuing institution recognizes it as a proxy transaction number, indexes the customer account record, and looks up the associated private key and customer-specific data. The institution computes a test code number using the same function and input parameters as the customer computer. The issuing institution compares the test code number with the code number embedded in the transaction number. If the two numbers match, the issuing institution accepts the transaction number as valid."

Applicant respectfully submits that while Franklin et al describe an online commerce card for online transactions, Franklin et al do not disclose or suggest an authorization of an off-line redemption of an issued certificate at a redemption location to a holder of the issued certificate located at said redemption location, based upon a communication from the remote location to a certificate authority of a redemption denomination and a first public key identifier from the issued certificate, and a private key provided by the holder, and a matching comparison of the redemption denomination, the first public key identifier, and the private key stored at the certificate authority. As well, it would therefore take significant modification and undue experimentation to meet Claim 1 and Claim 16, as amended.

Therefore, Applicant submits that Claim 1 and Claim 16, as amended, overcome the rejections under 35 U.S.C. § 102(b) as being anticipated by Franklin et al (6,006,831). As dependent claims 3-6, 8, 9, 11, and 13-15 depend  
5 from amended independent Claim 1, and as dependent claims 18-21, 23, 24, 26, and 28-30 depend from amended independent Claim 16, and inherently contain all the limitations of the claims they depend from, they are seen to be patentable as well.

10 **4-7. 35 U.S.C. § 103. Rejections.**

5. Claims 2, 10, 17 and 25 are rejected under 35 U.S.C. §103(a) as being unpatentable over Franklin et al (U.S. Patent No. 6,000,832).

As described above, Applicant has amended independent Claim 1, to claim a  
15 certificate system on a network, comprising:

a certificate authority connected to said network, said certificate authority adapted to allow the definition of a virtual certificate comprising a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

20 a certificate issuance module for creation of an issued certificate upon selectable acquisition of said virtual certificate by an acquirer user across said network, said issued certificate comprising said redemption denomination and said first public key identifier, said creation of said issued certificate comprising a private key assigned at time of said acquisition of said virtual certificate,  
25 wherein said redemption denomination, said first public key identifier, and said assigned private key are stored at said certificate authority in association with said issued certificate;

a certificate authentication module for authorization of an off-line redemption of said issued certificate at a redemption location to a holder of said  
30 issued certificate located at said redemption location, based upon a communication from said remote location to said certificate authority of said redemption denomination and said first public key identifier from said issued certificate, and said private key provided by said holder, and a matching

comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

means to cancel further redemption of said issued certificate at said certificate authority.

5

Also as described above, Applicant has also amended independent Claim 16, to claim a process within a transaction network, comprising the steps of:

defining a virtual certificate on a certificate authority, said defined virtual certificate comprised of a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

10

creating an issued certificate upon acquisition of said virtual certificate by an acquirer user on said transaction network, said issued certificate comprising said redemption denomination and said first public key identifier, said creation of said issued certificate comprising an establishment of a private key, said redemption denomination, said first public key identifier, and said established private key stored at said certificate authority in association with said issued certificate;

15

authorizing an off-line redemption of said issued certificate at a redemption location to a holder of said issued certificate, based upon redemption submittal at said redemption location of said redemption denomination and said first public key identifier from said issued certificate, and said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

20

canceling further redemption of said issued certificate at said certificate authority.

25

Applicant respectfully submits that while Franklin et al describe an online commerce card for online transactions, Franklin et al do not disclose or suggest an authorization of an off-line redemption of an issued certificate at a redemption location to a holder of the issued certificate located at said redemption location, based upon a communication from the remote location to a

30

certificate authority of a redemption denomination and a first public key identifier from the issued certificate, and a private key provided by the holder, and a matching comparison of the redemption denomination, the first public key identifier, and the private key stored at the certificate authority. As well, it would  
5 therefore take significant modification and undue experimentation to meet Claim 1 and Claim 16, as amended.

Therefore, Applicant submits that Claim 1 and Claim 16, as amended, overcome the rejections under 35 U.S.C. § 103(a) as being unpatentable over  
10 Franklin et al (6,006,831). As dependent claims 2 and 10 depend from amended independent Claim 1, and as dependent claims 17 and 25 depend from amended independent Claim 16, and inherently contain all the limitations of the claims they depend from, they are seen to be patentable as well.

15 6. Claims 7 and 22 are rejected under 35 U.S.C. §103(a) as being unpatentable over Franklin et al (U.S. Patent No. 6,000,832) in view of Lee et al (U.S. Patent No. 6,170,744 B1).

The Office Action states that “although Franklin et al do not disclose the  
20 “physical” generation of a certificate, Lee et al, figure 1, teach self-authenticating negotiable documents such that a physical certificate is generated by a user/customer for payment of off-line transactions. This certificate includes a bar code, element 110, containing information similar to the information contained in Franklin’s virtual certificate, such as amount of check  
25 (denomination), hash code, public key, and account number. Therefore, it is considered that it would have been obvious to one of ordinary skill in the art at the time of the invention to utilize the teachings of Lee et al in the system of Franklin et al so that a physical form of a certificate can be used in off-line transactions”.

30

As described above, Applicant has amended independent Claim 1, to claim a certificate system on a network, comprising:

a certificate authority connected to said network, said certificate authority adapted to allow the definition of a virtual certificate comprising a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

5 a certificate issuance module for creation of an issued certificate upon selectable acquisition of said virtual certificate by an acquirer user across said network, said issued certificate comprising said redemption denomination and said first public key identifier, said creation of said issued certificate comprising a private key assigned at time of said acquisition of said virtual certificate,  
10 wherein said redemption denomination, said first public key identifier, and said assigned private key are stored at said certificate authority in association with said issued certificate;

a certificate authentication module for authorization of an off-line redemption of said issued certificate at a redemption location to a holder of said  
15 issued certificate located at said redemption location, based upon a communication from said remote location to said certificate authority of said redemption denomination and said first public key identifier from said issued certificate, and said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and  
20 said private key stored at said certificate authority; and

means to cancel further redemption of said issued certificate at said certificate authority.

Also as described above, Applicant has also amended independent Claim 16,  
25 to claim a process within a transaction network, comprising the steps of:

defining a virtual certificate on a certificate authority, said defined virtual certificate comprised of a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

creating an issued certificate upon acquisition of said virtual certificate by  
30 an acquirer user on said transaction network, said issued certificate comprising said redemption denomination and said first public key identifier, said creation of said issued certificate comprising an establishment of a private key, said

redemption denomination, said first public key identifier, and said established private key stored at said certificate authority in association with said issued certificate;

authorizing an off-line redemption of said issued certificate at a redemption location to a holder of said issued certificate, based upon redemption submittal at said redemption location of said redemption denomination and said first public key identifier from said issued certificate, and said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

canceling further redemption of said issued certificate at said certificate authority.

While Lee et al describe self-authenticating negotiable document, Applicant respectfully submits that the self-authenticating negotiable document described by Lee et al is significantly different than the present invention, as claimed in Claim 1 and Claim 16, as amended. An overview of the self-authenticating negotiable document, as disclosed by Lee et al, is seen at least in the Abstract, wherein:

"A self-authenticating document is created by providing a one-way hash value in a symbol creation process, and then using a public key to decrypt data of the self-authenticating document. Raw data to be provided with the self-authenticating document is received; and an account digital signature key is retrieved and used to sign the raw data. A non-repudiation hash value from a previously-created self-authenticating document is utilized, and the raw data and the digital signature key is combined with the hash value to create a new hash value for the self-authenticating document. The hashed data is then encrypted, and any non-encrypted fields are merged in to create a full data packet. The full data packet is used to provide a self-authenticating symbol, such as a bar code label, on the self-authenticating document. The self-authenticating

code is used during a document verification step to ensure that the document is genuine. The non-encrypted data within the self-authenticating code contains flags indicating which public key should be used to decrypt the encrypted data within the self-authenticating code. After decryption, a checksum is performed and compared against a checksum value stored in the decrypted portion of the self-authenticating code. If they match, and if a digital signature within the self-authenticating code is verified using an appropriate public key, the document is determined to be authentic."

While the self-authentication negotiable document described by Lee et al includes a public key to decrypt data of the self-authenticating document, Applicant submits that Lee et al do not disclose or suggest an authorization of an off-line redemption of an issued certificate at a redemption location to a holder of the issued certificate located at said redemption location, based upon a communication from the remote location to a certificate authority of a redemption denomination and a first public key identifier from the issued certificate, and a private key provided by the holder, and a matching comparison of the redemption denomination, the first public key identifier, and the private key stored at the certificate authority.

Furthermore, neither Franklin et al nor Lee et al contain any suggestion, express or implied, that they be combined, or that they be combined in the manner suggested. As well, it would therefore take significant modification and undue experimentation to meet Claim 1 and Claim 16, as amended.

Therefore, Applicant submits that Claim 1 and Claim 16, as amended, overcome the rejections under 35 U.S.C. § 103(a) as being unpatentable over Franklin et al (6,006,831) in view of Lee et al. As dependent claim 7 depends from amended independent Claim 1, and as dependent claim 22 depends from amended independent Claim 16, and inherently contain all the limitations of the claims they depend from, they are seen to be patentable as well.

7. Claims 12 and 27 are rejected under 35 U.S.C. §103(a) as being unpatentable over Franklin et al (U.S. Patent No. 6,000,832) in view of Larsson et al (U.S. Patent No. 5,379,344).

5

The Office Action states that "although Franklin et al do not teach generating a new key for each issued certificate, Larsson et al teach smart card device wherein each new certificate, a new private key is generated. Therefore, it is considered that it would have been obvious to one of ordinary skill in the art at the time of the invention to utilize generating new keys with each new certificate/transaction as this would increase the security of the certificate, making it less likely to forge a certificate".

10

As described above, Applicant has amended independent Claim 1, to claim a certificate system on a network, comprising:

15

a certificate authority connected to said network, said certificate authority adapted to allow the definition of a virtual certificate comprising a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

20

a certificate issuance module for creation of an issued certificate upon selectable acquisition of said virtual certificate by an acquirer user across said network, said issued certificate comprising said redemption denomination and said first public key identifier, said creation of said issued certificate comprising a private key assigned at time of said acquisition of said virtual certificate, wherein said redemption denomination, said first public key identifier, and said assigned private key are stored at said certificate authority in association with said issued certificate;

25

a certificate authentication module for authorization of an off-line redemption of said issued certificate at a redemption location to a holder of said issued certificate located at said redemption location, based upon a communication from said remote location to said certificate authority of said redemption denomination and said first public key identifier from said issued

30

certificate, and said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

means to cancel further redemption of said issued certificate at said  
5 certificate authority.

Also as described above, Applicant has also amended independent Claim 16, to claim a process within a transaction network, comprising the steps of:

defining a virtual certificate on a certificate authority, said defined virtual  
10 certificate comprised of a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

creating an issued certificate upon acquisition of said virtual certificate by an acquirer user on said transaction network, said issued certificate comprising said redemption denomination and said first public key identifier, said creation  
15 of said issued certificate comprising an establishment of a private key, said redemption denomination, said first public key identifier, and said established private key stored at said certificate authority in association with said issued certificate;

authorizing an off-line redemption of said issued certificate at a  
20 redemption location to a holder of said issued certificate, based upon redemption submittal at said redemption location of said redemption denomination and said first public key identifier from said issued certificate, and said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and said private key  
25 stored at said certificate authority; and

canceling further redemption of said issued certificate at said certificate authority.

While Larsson et al describe smart card validation device and method,  
30 Applicant respectfully submits that the smart card validation device and method described by Lee et al is significantly different than the present invention, as claimed in Claim 1 and Claim 16, as amended. An overview of the smart card

validation device and method, as disclosed by Larsson et al, is seen at least in the Abstract, wherein:

5 "A validation device (2) for a smart card (1) of the kind having unprotected data storage memory (4) and protected data storage memory (5) selectively accessible by means of a user access code. The device (2) performs an encryption upon identification data to produce the user access code and reads identification data from the unprotected memory (4) for further encryption. The access code is supplied to the  
10 smart card (1) and selected data from said protected memory (5) is read for encryption to produce validating data. A comparator (8) compares the identification data with the validating data and rejects the smart card (1) if the data do not agree and establishes access to said protected memory (5) if the data do agree."

15 While the smart card validation device and method described by Larsson et al includes a user access code, Applicant submits that Larsson et al do not disclose or suggest an authorization of an off-line redemption of an issued certificate at a redemption location to a holder of the issued certificate located at  
20 said redemption location, based upon a communication from the remote location to a certificate authority of a redemption denomination and a first public key identifier from the issued certificate, and a private key provided by the holder, and a matching comparison of the redemption denomination, the first public key identifier, and the private key stored at the certificate authority.

25 Furthermore, neither Franklin et al nor Larsson et al contain any suggestion, express or implied, that they be combined, or that they be combined in the manner suggested. As well, it would therefore take significant modification and undue experimentation to meet Claim 1 and Claim 16, as amended.

30 Therefore, Applicant submits that Claim 1 and Claim 16, as amended, overcome the rejections under 35 U.S.C. § 103(a) as being unpatentable over

Franklin et al (6,006,831) in view of Larsson et al. As dependent claim 12 depends from amended independent Claim 1, and as dependent claim 27 depends from amended independent Claim 16, and inherently contain all the limitations of the claims they depend from, they are seen to be patentable as well.

8. Applicant has also amended the Specification and Claims, as shown above, to correct grammatical errors.

### CONCLUSION

Applicant therefore respectfully submits that Claims 1-30, as amended, overcome the rejections set forth in the Office Action. Applicant also submits that the amendments do not introduce new matter into the Application. Based on the foregoing, Applicant considers the invention to be in condition for allowance. Applicant earnestly solicits the Examiner's withdrawal of the rejections set forth in the prior Office Action, such that a Notice of Allowance is forwarded to Applicant, and the present application is therefore allowed to issue as a United States patent.

Respectfully Submitted,



Michael A. Glenn  
Reg. No. 30,176

Customer No. 22862

## Marked-up Version to Show Changes in the Specification

Please amend the specification as follows:

5 On page 5, lines 20-30 of the Application as filed;

10 In an alternate embodiment of a conventional online gift certificate site, a buyer may purchase a “generic” gift certificate, which is then typically given as a gift to a recipient, whereby the generic gift certificate is supplied with a tracking number (which may be sent to a recipient, or may be e-mailed to the recipient[?]). The recipient may then log on to the gift certificate site, and “redeem” the generic gift certificate by selecting one or more specific gift certificates, which in sum are equal to the designated value of the original generic certificate. However, as with other online business which offer paper  
15 based certificates for sale, the specific certificates are limited to an actual inventory of paper-based gift certificates which are available at that site. Upon redemption of the generic certificate, the specific certificate or certificates are then physically sent to the redeemer.

20 On page 12, lines 5-10 of the Application as filed;

**Acquisition of Certificates and Establishment of Keys.** Figure 3 is a schematic view of an acquisition transaction 72 for a single-use certificate 60. [identification packet 74.] During an acquisition transaction 72, an acquirer user  
25 ACQ typically provides a means to purchase a certificate 60, an authorization to purchase during a subsequent redemption transaction 104 (FIG. 4), or otherwise qualifies for issuance of the acquired certificate 60.

On page 26, lines 20-31 of the Application as filed;

30

**Certificate Redemption.** Figure 8 is a detailed schematic block diagram 174 of redeemer facility options. A redemption clerk RC (*e.g.* such as a sales clerk at a redemption location), establishes electronic communication with a certificate authority 12 through redeemer facilities 38. As seen in Figure 1, the  
35 redeemer facilities 38 are typically accessed through a redeemer computer

terminal 36, a redeemer POS terminal 40, or by a telephone 44 (either by using a keypad driven menu, or through a live operator intermediary 14). One or more redeemer terminals 36, point of sale terminals 40, and/or telephonic devices 40 may be located at the redemption location RL, and may include a variety of wireless network communications, such as a localized wireless network at the redemption location RL, or as remote wireless connections across a network 192 (FIG. 9) to the certificate authority 12, such as to the authorization server 16.

On page 29, lines 18-29 of the Application as filed;

The issuer design module 200 typically includes selection of various design elements 62, such as through add design element control 122a, design library control 122b, and upload design control 122c. Attributes for a design are preferably set by attribute control 208. A design element 62 is preferably activated by control 210. A design element 62 which is not needed may be deleted by deletion control 212. The issuer design module 200 preferably includes indicia selection control 122d, in which the issuer user may define the number and type of certificate identification indicia 88 (FIG. 3) to be displayed on an acquired certificate 60, such as a human readable serial code 68, or machine readable indicia 70. The redemption rule module 202 typically includes user selectable expiration limitations 124a, location selection 124b, or other redemption rules 124c. As well, other issuer entered restrictions may be entered, such as availability 126a, or other restrictions 126n.

## Marked-up Version to Show Changes in the Claims

Please amend Claims 1, 4-8, and 16-23 as follows:

5 Claim 1. (Amended) A certificate system on a network, comprising:

a certificate authority connected to said network, said certificate authority adapted to allow the definition of a virtual certificate comprising a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

10 a certificate issuance module for creation of an issued certificate upon selectable acquisition of said virtual certificate by an acquirer user across said network, said issued certificate [including] comprising said redemption denomination and said first public key identifier, said creation of said issued certificate [including] comprising a private key assigned at time of said  
15 acquisition of said virtual certificate, wherein said redemption denomination, said first public key identifier, and said assigned private key are stored at said certificate authority in association with said issued certificate;

a certificate authentication module for authorization of [a] an off-line redemption of said issued certificate at a redemption location to a holder of said  
20 issued certificate located at said redemption location, based upon [redemption submittal] a communication from said <sup>denomination</sup> remote location to said certificate authority of said redemption denomination [,] and said first public key identifier from said issued certificate, and said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and  
25 said private key stored at said certificate authority; and

means to cancel further redemption of said issued certificate at said certificate authority.

4. (Amended) The certificate system of Claim 3, wherein said required  
30 submittal of said payment agent for said acquirer user [includes] comprises an authorization to transfer funds from said payment agent for said acquirer upon creation of said issued certificate.

5. (Amended) The certificate system of Claim 3, wherein said required submittal of said payment agent for said acquirer user [includes] comprises an authorization to transfer funds from said payment agent for said acquirer upon redemption of said issued certificate.

6. (Amended) The certificate system of Claim 1, wherein said certificate issuance module [includes] comprises means to deliver said redemption denomination, said first public key identifier, and said [entered] assigned private key to said acquirer user.

7. (Amended) The certificate system of Claim 6, wherein said means to deliver said redemption denomination, said first public key identifier, and said [entered] assigned private key to said acquirer user comprises a printed form of said issued certificate.

8. (Amended) The certificate system of Claim 6, wherein said means to deliver said redemption denomination, said first public key identifier, and said [entered] assigned private key to said acquirer user comprises an electronic form of said issued certificate.

16. (Amended) A process within a transaction network, comprising the steps of:  
defining a virtual certificate on a certificate authority, said defined virtual certificate comprised of a redemption denomination defined by an issuer user, and a first public key identifier defined by said certificate authority;

creating an issued certificate upon acquisition of said virtual certificate by an acquirer user on said transaction network, said issued certificate [including] comprising said redemption denomination and said first public key identifier, said creation of said issued certificate [including] comprising an establishment of a private key, said redemption denomination, said first public key identifier, and said established private key stored at said certificate authority in association with said issued certificate;

authorizing [a] an off-line redemption of said issued certificate at a redemption location to a holder of said issued certificate, based upon redemption submittal at said redemption location of said redemption denomination[,] and said first public key identifier from said issued certificate,  
5 and said private key provided by said holder, and a matching comparison of said redemption denomination, said first public key identifier, and said private key stored at said certificate authority; and

canceling further redemption of said issued certificate at said certificate authority.

10

17. (Amended) The process of Claim 16, wherein said step of defining said virtual certificate, wherein said defined virtual certificate [includes] comprises a second public key identifier defined by said issuer user, wherein said step of creating said issued certificate includes the storage of said second public key  
15 identifier at said certificate authority, and wherein said step of authorizing said redemption of said issued certificate [includes] comprises a submittal of said second public key identifier, and a matching comparison to said second public key identifier stored at said certificate authority.

20 18. (Amended) The process of Claim 16, wherein said step of creation of said issued certificate [includes] comprises the submittal of a payment agent by said acquirer user.

25 19. (Amended) The process of Claim 18, wherein said submittal of said payment agent for said acquirer user [includes] comprises an authorization to transfer funds from said payment agent for said acquirer during said step of creation of said issued certificate.

30 20. (Amended) The process of Claim 18, wherein said submittal of said payment agent for said acquirer user [includes] comprises an authorization to transfer funds from said payment agent for said acquirer during said step of redemption of said issued certificate.

21. (Amended) The process of Claim 16, wherein said step of creation of said issued certificate [includes] comprises a delivery of said redemption denomination, said first public key identifier, and said [entered] established  
5 private key to said acquirer user.

22. (Amended) The process of Claim 21, wherein said delivered redemption denomination, said first public key identifier, and said [entered] established private key to said acquirer user are included in a printed form of said issued  
10 certificate.

23. (Amended) The process of Claim 21, wherein said delivered redemption denomination, said first public key identifier, and said [entered] established private key to said acquirer user are included in an electronic form of said  
15 issued certificate.